§170.315(g)(9) Application access — all data request

2015 Edition Cures Update CCG

Version 1.0 Updated on 06-15-2020

Revision History

Version #	Description of Change	Version Date
1.0	Initial Publication	06-15-2020

Regulation Text

Regulation Text

§ 170.315 (g)(9) *Application access – all data request—*

The following technical outcome and conditions must be met through the demonstration of an application programming interface.

(i) *Functional requirements.*

(A) (1) Respond to requests for patient data (based on an ID or other token) for all of the data classes expressed in the standards in § 170.213 at one time and return such data (according to the specified standards, where applicable) in a summary record formatted in accordance with § 170.205(a)(4) and (5) following the CCD document template, and as specified in paragraphs (g)(9)(i)(A)(*3*)(*i*) through (*iii*) of this section, or

(1) The Common Clinical Data Set in accordance with paragraphs (g)(9)(i)(A)(*3*)(*i*) through (*iv*) of this section for the period until May 2, 2022, and

(2) The following data classes:

(i) Assessment and plan of treatment. In accordance with the "Assessment and Plan Section (V2)" of the standards specified in § 170.205(a)(4); or in accordance with the "Assessment Section (V2)" and "Plan of Treatment Section (V2)" of the standards specified in § 170.205(a)(4).

(ii) Goals. In accordance with the "Goals Section" of the standard specified in § 170.205(a)(4).

(iii) Health concerns. In accordance with the "Health Concerns Section" of the standard specified in § 170.205(a)(4).

(iv) Unique device identifier(s) for a patient's implantable device(s). In accordance with the "Product Instance" in the "Procedure Activity Procedure Section" of the standard specified in § 170.205(a)(4).

(B) Respond to requests for patient data associated with a specific date as well as requests for patient data within a specified date range.

(ii) *Documentation—*

(A) The API must include accompanying documentation that contains, at a minimum:

(1) API syntax, function names, required and optional parameters and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.

(2) The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).

(3) Terms of use. The terms of use for the API must be provided, including, at a minimum, any associated developer policies and required developer agreements.

(B) The documentation used to meet paragraph (g)(9)(ii)(A) of this section must be available via a publicly accessible hyperlink.

Standard(s) Referenced

Paragraph (g)(9)(i)(A)

§ 170.213 United States Core Data for Interoperability (USCDI) Version 1

§ 170.205(a)(4) Health Level 7 (HL7®) Implementation Guide for CDA Release 2 Consolidation CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use Release 2.1 C-CDA 2.1, August 2015, June 2019 (with Errata)

§ 170.205(a)(5) HL7® CDA R2 IG: C-CDA Templates for Clinical Notes R2.1 Companion Guide, Release 2, October 2019, IBR approved for § 170.205(a)(5)

Certification Companion Guide: Application access — all data request

This Certification Companion Guide (CCG) is an informative document designed to assist with health IT product development. The CCG is not a substitute for the *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program* Final Rule (ONC Cures Act Final Rule). It extracts key portions of the rule's preamble and includes subsequent clarifying interpretations. To access the full context of regulatory intent please consult the ONC

Cures Act Final Rule or other included regulatory reference. The CCG is for public use and should not be sold or redistributed.

Link to Final Rule Preamble

Edition Comparision	Gap Certification Eligible	Base EHR Definition	In Scope for CEHRT Definition
New	No	Included	Yes

Certification Requirements

Privacy and Security: This certification criterion was adopted at § 170.315(g)(9). As a result, an ONC-ACB must ensure that a product presented for certification to this criterion includes the privacy and security criteria (adopted in § 170.315(d)) within the overall scope of the certificate issued to the product.

- The privacy and security criteria (adopted in § 170.315(d)) do not need to be explicitly tested with this specific criterion unless it is the only criterion for which certification is requested.
- As a general rule, a product presented for certification only needs to be tested once to each applicable privacy and security criterion (adopted in § 170.315(d)) so long as the health IT developer attests that such privacy and security capabilities apply to the full scope of capabilities included in the requested certification. However, exceptions exist for § 170.315(e)(1) "VDT" and (e)(2) "secure messaging", which are explicitly stated.

Table for Privacy and Security

- If choosing Approach 1:
  - Authentication, access control, and authorization (§ 170.315(d)(1))
  - Trusted connection (§ 170.315(d)(9))
  - Either auditable events and tamper-resistance (§ 170.315(d)(2)) or auditing actions on health information (§ 170.315(d)(10)).
  - Encrypt authentication credentials (§ 170.315(d)(12))
  - Multi-factor authentication (MFA) (§ 170.315(d)(13))
- If choosing Approach 2:

- For each applicable P&S certification criterion not certified for Approach 1, the health IT developer may certify using system documentation which is sufficiently detailed to enable integration such that the Health IT Module has implemented service interfaces the Health IT Module to access external services necessary to meet the requirements of the P&S certification criterion. Please see the ONC Cures Act Final Rule at 85 FR 25710 for additional clarification.

Design and Performance: The following design and performance certification criteria (adopted in § 170.315(g)) must also be certified in order for the product to be certified.

- When a single quality management system (QMS) is used, the QMS only needs to be identified once. Otherwise, the QMS' need to be identified for every capability to which it was applied.
- When a single accessibility-centered design standard is used, the standard only needs to be identified once. Otherwise, the accessibility-centered design standards need to be identified for every capability to which they were applied; or, alternatively the developer must state that no accessibility-centered design was used.
- Consolidated-Clinical Document Architecture (C-CDA) creation performance (§ 170.315(g)(6)) does not need to be explicitly tested with this criterion unless it is the only criterion within the scope of the requested certification that includes C-CDA creation capabilities. Note that the application of § 170.315(g)(6) depends on the C-CDA templates explicitly required by the C-CDA-referenced criterion or criteria included within the scope of the certificate sought. Please refer to the C-CDA Creation Performance Certification Companion Guide for more details.

Table for Design and Performance

- Quality management system (§ 170.315(g)(4))
- Accessibility-centered design (§ 170.315(g)(5))
- Consolidated CDA creation performance (§ 170.315(g)(6))

Technical Explanations and Clarifications

Applies to entire criterion

Clarifications:

- *Security:*
  - For the purposes of certification there is no conformance requirement related to the registration of third-party applications that use the application programming interfaces (APIs). If a Health IT module requires registration as a pre-condition for accessing the APIs, then, the process must be clearly specified in the API documentation as required by the criterion. We strongly believe that registration should not be used to block information sharing via APIs.
  - This criterion does not currently include any security requirements beyond the privacy and security approach detailed above, but we encourage organizations to follow security best practices and implement security controls, such as penetration testing, encryption, audits, and monitoring as appropriate. We expect health IT developers to include information on how to securely use their APIs in the public documentation required by the certification criteria and follow industry best practices. [see also 80 FR 62676 and 85 FR 25642]
  - We strongly encourage developers to build security into their APIs following best practice guidance, such as the Department of Homeland Security's Build Security In initiative.[1] [see also 80 FR 62677]
  - A "trusted connection" means the link is encrypted/integrity protected according to § 170.210(a)(2) or (c)(2). As such, we do not believe it is necessary to specifically name HTTPS and/or SSL/TLS as this standard already covers encryption and integrity protection for data in motion. [see also 80 FR 62676]
  - APIs could be used when consent or authorization by an individual is required. In circumstances where there is a requirement to document a patient's request or particular preferences, APIs can enable compliance with documentation requirements. The Health Insurance Portability and Accountability Act of 1996 Privacy Rule[2] permits the use of electronic documents to qualify as writings for the purpose of proving signature, e.g., electronic signatures. [see also 80 FR 62677]
- The audit record should be able to distinguish the specific user who accessed the data using a third-party application through the certified API to meet the requirements of § 170.315(d)(2) or (d)(10).
- A health IT developer must demonstrate the API functionality of the Health IT Module properly performs consistent with this certification criterion's requirements. As part of the demonstration process, a health IT developer is permitted, but is not limited to, using existing tools for creating its own app or "client" to interact with the API or using a third-party application for demonstration.

- By requiring that documentation and terms of use be open and transparent to the public by requiring a hyperlink to such documentation to be published with the product on the ONC Certified Health IT Product List, we hope to encourage an open ecosystem of diverse and innovative applications that can successfully and easily interact with different Health IT Modules' APIs. [see also 80 FR 62679 and 85 FR 25642]
- By no later than November 2, 2020, a Certified API Developer with Health IT Module(s) certified to the certification criteria in § 170.315(g)(7), (8), or (9) must comply with paragraph (a) of this section, including revisions to their existing business and technical API documentation and make such documentation available via a publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps.

[1] https://buildsecurityin.us-cert.gov/
[2] 45 CFR Part 160 and Part 164, Subparts A and E

Paragraph (g)(9)(i)(A)

Technical outcome – The API must be able to respond to requests for patient data (using an ID or other token) for all of the data categories specified in the United States Core Data for Interoperability Standard (USCDI) at one time in a summary record formatted according to the Consolidated CDA Release 2.1 Continuity of Care Document (CCD) template.

Clarifications:

- Please refer to the USCDI for the data standards that are required.
- The technology specifications should be designed and implemented in such a way as to return meaningful responses to queries, particularly with regard to exceptions and exception handling, and should make it easy for applications to discover what data exists for the patient. [see also 80 FR 62678]
- The term "token" that is used here is not to be interpreted as the token in the OAuth2 workflow, but simply as something that would uniquely identify a patient.
- In order to mitigate potential interoperability errors and inconsistent implementation of the HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes, Draft Standard for Trial Use, Release 2.1, ONC assesses, approves, and incorporates corrections as part of required testing and certification to this criterion. [see Frequently Asked

Questions #51] Certified health IT adoption and compliance with the following corrections are necessary because they implement updates to vocabularies, update rules for cardinality and conformance statements, and promote proper exchange of C-CDA documents. There will be a 90-day delay from the time the CCG has been updated with the ONC-approved corrections to when compliance with the corrections will be required to pass testing (i.e., C-CDA 2.1 Validator).There will be an 18-month delay before a finding of a correction's absence in certified health IT during surveillance would constitute a non-conformity under the Program.

Paragraph (g)(9)(i)(B)

Technical outcome – The API must be able to respond to requests for patient data associated with a specific date as well as with a specific date range.

Clarifications:

- Health IT returning an entire patient record that does not reflect the specific date or date range requested is not permissible when a specific date or date range is requested. [see also 80 FR 62678]
- The developer can determine the method and the amount of data by which the health IT uniquely identifies a patient. [see also 80 FR 62678]
- The API must be able to send, at minimum all required data for a specified date range(s). We acknowledge that there will be organizational policies and/or safety best practices that will dictate additional data to be sent and when data is considered complete and/or ready for being sent. This should be appropriately described in the API documentation.
- The approach used to provide the CCD document(s) is set by the API. An approach based on providing one or more CCD documents matching to the patient's selected date or date range is a valid approach.

Paragraph (g)(9)(ii)(A)(*1*)

Technical outcome – The API must include accompanying documentation which contains API syntax, function names, required and optional parameters and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.

Clarifications:

- No additional clarifications available.

Paragraph (g)(9)(ii)(A)(*2*)

Technical outcome – The API must include accompanying documentation, which contains software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).

Clarifications:

- No additional clarifications available.

Paragraph (g)(9)(ii)(B)

Technical outcome – The documentation used to meet the provisions in (g)(9)(ii)(A)(*1*)-(*3*) must be available through a publicly accessible hyperlink.

Clarifications:

- The hyperlink provided for all of the documentation referenced by provision (g)(9)(ii)(A) must reflect the most current version of the Health IT developer's documentation.
- All of the documentation referenced by provision (g)(9)(ii)(A) must be accessible to the public via a hyperlink without additional access requirements, including, without limitation, any form of registration, account creation, "click-through" agreements, or requirement to provide contact details or other information prior to accessing the documentation.

Content last reviewed on June 22, 2020